Ex. E - Claim Chart
U.S. Patent No. 9,600,661

US009600661B2

(12) **United States Patent**
Safa

(10) **Patent No.: US 9,600,661 B2**
(45) **Date of Patent: Mar. 21, 2017**

(54) **SYSTEM AND METHOD TO SECURE A COMPUTER SYSTEM BY SELECTIVE CONTROL OF WRITE ACCESS TO A DATA STORAGE MEDIUM**

(75) Inventor: **John Safa**, Nottingham (GB)

(73) Assignee: **Drive Sentry Limited**, Berkshire (GB)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 503 days.

(21) Appl. No.: **11/292,910**

(22) Filed: **Dec. 1, 2005**

(65) **Prior Publication Data**

US 2007/0130433 A1 Jun. 7, 2007

(51) **Int. Cl.**
G06F 12/00 (2006.01)
G06F 21/52 (2013.01)

(52) **U.S. Cl.**
CPC ***G06F 21/52*** (2013.01)

(58) **Field of Classification Search**
CPC G06F 12/14; G06F 21/52
USPC 711/163
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,825,877 A 10/1998 Dan et al.
5,974,549 A * 10/1999 Golan 726/23
6,308,274 B1 10/2001 Swift
6,922,781 B1 * 7/2005 Shuster 713/165
6,941,470 B1 9/2005 Jooste
6,978,366 B1 * 12/2005 Ignatchenko et al. 713/166
7,681,237 B1 * 3/2010 Spiegel 726/24
(Continued)

FOREIGN PATENT DOCUMENTS

GB 2402515 A * 12/2004
JP 08044630 A 2/1996
(Continued)

OTHER PUBLICATIONS

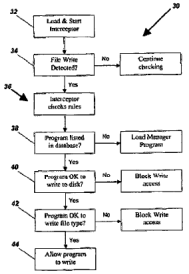
FileMerlin?. Conversion Library and API for Developers [online]. Advanced Computer Innovations, Inc., 2004 [retrieved on Jan. 28, 2008]. Retrieved from the Internet: <URL:http://web.archive.org/web/20040810113019/file-convert.com/fmdvref.htm>.*
(Continued)

Primary Examiner — Larry Mackall
(74) *Attorney, Agent, or Firm* — Ted Sabety; Sabety +associates, PLLC

(57) **ABSTRACT**

The present invention relates to a method and system of controlling the writing of data to a computer storage medium such as a hard drive in a computer system in order to prevent viruses or similar program code from being saved on such medium. Upon the computer system initiating a request to write data to the medium, the application embodying the method and system checks the identity of the running application requesting to perform the write. The method and system then checks a rule database to determine if such requesting application has permission to write to the medium. The system can also check that the data file type that the application seeks to write is a permitted type for that application. In response to the output of the database check, the requested write is allowed to proceed or is blocked. In the absence of a rule, the system presents the request to the computer user. The user can either grant permission or block, and such response can be included in the rule database. User responses can be collected from many instances of the invention and the collective response of users presented to a user.

58 Claims, 3 Drawing Sheets



Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:	Sophos offers various software that performs the method of claim 16. Specifically, Sophos offers many applications to protect against electronic threats such as viruses, ransomware, malware, and the like. That software includes features such as Sophos Anti-Virus, Sophos Behavior Monitoring, and/or Sophos Live Protection. For example, the infringing products that incorporate those features include Endpoint Security and Control, Central Endpoint Protection, Intercept X, Intercept X Advanced, Intercept X Advanced with EDR, Home, and Home Premium. Sophos Endpoint Security and Control is an integrated suite of security software. **Sophos Anti-Virus** detects and cleans up viruses, Trojans, worms, and spyware, as well as adware and other potentially unwanted applications. Our HIPS (Host Intrusion Prevention System) technology can also protect your computer from suspicious files and rootkits. In addition, Malicious Traffic Detector can detect communications between your computer and command and control servers involved in a botnet or other malware attack. **Sophos Behavior Monitoring** uses our HIPS technology to protect Windows computers from unidentified or "zero-day" threats and suspicious behavior. **Sophos Live Protection** improves detection of new malware without the risk of unwanted detections. This is achieved by doing an instant lookup against the very latest known malware. When new malware is identified, Sophos can send out updates within seconds. **Sophos Web Protection** provides enhanced protection against web threats by preventing access to locations that are known to host malware. It blocks endpoints' access to such sites by performing a real-time lookup against Sophos's online database of malicious websites. It also scans downloaded data and files and checks file reputation. **Sophos Application Control** blocks unauthorized applications such as Voice over IP, instant messaging, file sharing, and game software. **Sophos Device Control** blocks unauthorized external storage devices and wireless connection technologies. **Sophos Data Control** prevents the accidental leakage of personally-identifiable information from managed computers. **Sophos Web Control** provides protection, control, and reporting for computers that are located, or roam, outside the corporate network. **Sophos Client Firewall** prevents worms, Trojans, and spyware from stealing and distributing sensitive information, and also prevents intrusion from hackers. **Sophos AutoUpdate** offers fail-safe updating and can throttle bandwidth when updating over low-speed network connections. **Sophos Tamper Protection** prevents unauthorized users (users with limited technical knowledge) and known malware from uninstalling Sophos security software or disabling it through the Sophos Endpoint Security and Control interface. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 2

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:	Relevant features discussed in this chart span the software of Endpoint Security and Control, Intercept X, Intercept X Advanced, Intercept X Advanced with EDR, Central Endpoint, Home, and Home Premium as shown in this charts. Upon information and belief, Endpoint Security and Control is an earlier iteration of the Intercept X & Central Endpoint Suite.

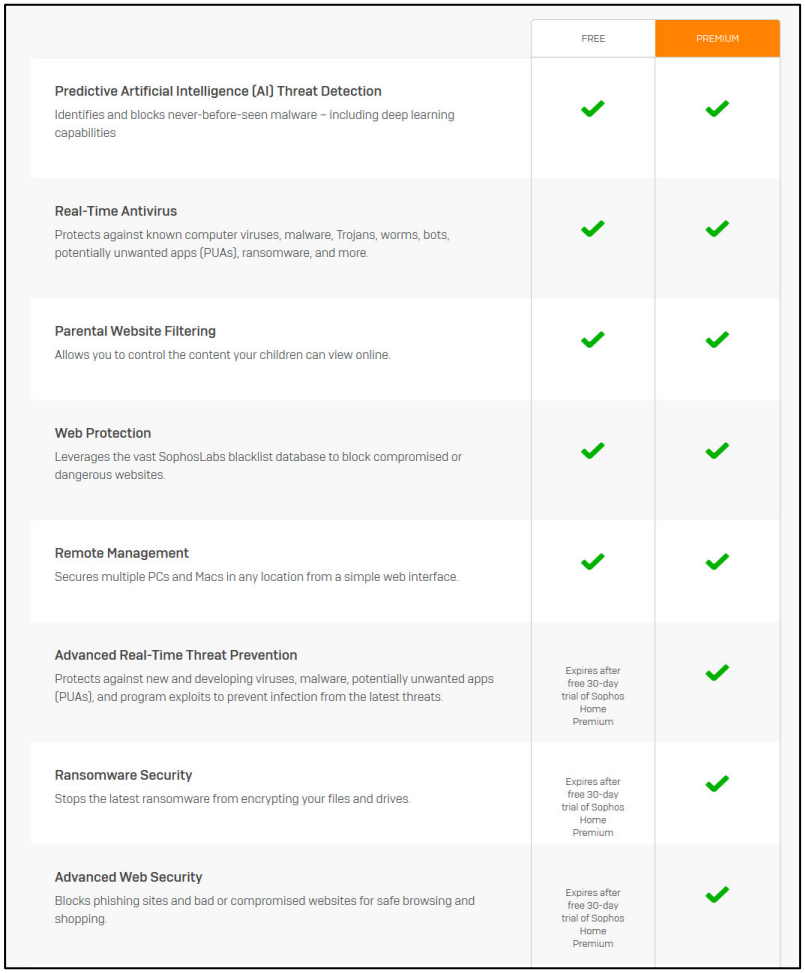
Intercept X & Central Endpoint Protection Overview

Managed by Sophos Central

		SKU	CENTRAL ENDPOINT PROTECTION	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH EDR
PREVENT	ATTACK SURFACE REDUCTION	Web Security	✓	✓	✓
		Download Reputation	✓	✓	✓
		Web Control / Category-based URL Blocking	✓	✓	✓
		Peripheral Control (e.g. USB)	✓	✓	✓
		Application Control	✓	✓	✓
	BEFORE IT RUNS ON DEVICE	Deep Learning Malware Detection		✓	✓
		Anti-Malware File Scanning	✓	✓	✓
		Live Protection	✓	✓	✓
		Pre-execution Behavior Analysis (HIPS)	✓	✓	✓
		Potentially Unwanted Application (PUA) Blocking	✓	✓	✓
		Intrusion Prevention System (IPS, coming 2020)	✓	✓	✓
	STOP RUNNING THREAT	Data Loss Prevention	✓	✓	✓
		Runtime Behavior Analysis (HIPS)	✓	✓	✓
		Antimalware Scan Interface (AMSI)	✓	✓	✓
		Malicious Traffic Detection (MTD)	✓	✓	✓
		Exploit Prevention (details on page 2)		✓	✓
		Active Adversary Mitigations (details on page 2)		✓	✓
		Ransomware File Protection (CryptoGuard)		✓	✓
		Disk and Boot Record Protection (WipeGuard)		✓	✓
		Man-in-the-Browser Protection (Safe Browsing)		✓	✓
		Enhanced Application Lockdown		✓	✓
DETECT AND INVESTIGATE	DETECT	Cross Estate Threat Searching (inc. files, scripts)			✓
		Suspicious Events Detection and Prioritization			✓
	INVESTIGATE	Threat Cases (Root Cause Analysis)		✓	✓
		Deep Learning Malware Analysis			✓
		Advanced On-demand SophosLabs Threat Intelligence			✓
		Forensic Data Export			✓
RESPOND	REMEDIATE	Automated Malware Removal	✓	✓	✓
		Synchronized Security Heartbeat	✓	✓	✓
		Sophos Clean		✓	✓
		On-demand Endpoint Isolation			✓
		Single-click "Clean and Block"			✓

https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-endpoint-license-guide.pdf

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:	This chart shows an overview of the Sophos Home versus Premium editions.  https://home.sophos.com/en-us/free-anti-virus-windows.aspx

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:	Sophos's software operates and runs on a computer such as a PC, Mac, or Server with mass storage device such as a hard disk or memory. The software controls write access to the computer's storage device to prevent malicious files from being written to the device, which is a central purpose of the software sold by Sophos. As shown below, Sophos's software analyzes applications running on the computer and blocks activity of the applications that appear to be malicious, including blocking write access to the storage device. Malicious and suspicious behavior detection Suspicious behavior detection uses Sophos's Host Intrusion Prevention System (HIPS) to dynamically analyze the behavior of all programs running on the computer to detect and block activity that appears to be malicious. Suspicious behavior may include changes to the registry that could allow a virus to run automatically when the computer is restarted. Suspicious behavior detection watches all system processes for signs of active malware, such as suspicious writes to the registry or file copy actions. It can be set to warn the administrator and/or block the process. Malicious behavior detection dynamically analyses all programs running on the computer to detect and block activity that is known to be malicious. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 25-26

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[a] detecting using a process operating in kernel mode monitoring file system access an attempt by the application to write data of a designated file type to said data storage device;	Sophos's software performs the step of detecting using a process operating in kernel mode monitoring file system access an attempt by the application to write data of a designated file type to said data storage device. For example, Sophos's "malicious behavior detection" analyses programs running on the computer to detect and block known malicious activity, including attempts to write data to the storage device. As shown below, using Sophos's Behavior Monitoring, Sophos's "suspicious behavior detection analyzes the behavior of program and watches for signs of malware, such as suspicious writes to the registry or file copy actions." Malicious and suspicious behavior detection Suspicious behavior detection uses Sophos's Host Intrusion Prevention System (HIPS) to dynamically analyze the behavior of all programs running on the computer to detect and block activity that appears to be malicious. Suspicious behavior may include changes to the registry that could allow a virus to run automatically when the computer is restarted. Suspicious behavior detection watches all system processes for signs of active malware, such as suspicious writes to the registry or file copy actions. It can be set to warn the administrator and/or block the process. Malicious behavior detection dynamically analyses all programs running on the computer to detect and block activity that is known to be malicious. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 25-26

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[a] detecting using a process operating in kernel mode monitoring file system access an attempt by the application to write data of a designated file type to said data storage device;	As another example, Sophos's "on-access scanning," detects attempts by applications to write data to said storage devices. For example, on-access scanning detects attempts to open, save, copy or rename a file, which necessarily includes an attempt by the application to write data to said storage medium. Further, "on-access scanning" may be set to "check files on write." On-access scanning On-access scanning is your main method of protection against viruses and other threats. Whenever you open, save, copy or rename a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your computer or has been authorized for use. For more information, see Configure on-access scanning (page 7). 2. To change when on-access scanning occurs, under **Check files on**, set the options as described below. Option / Description Read — Scan files when they are copied, moved, or opened. Rename — Scan files when they are renamed. Write — Scan files when they are saved or created. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 7-8

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[a] detecting using a process operating in kernel mode monitoring file system access an attempt by the application to write data of a designated file type to said data storage device;	As noted in the previous slides for limitation 16[a], Sophos's software detects attempts by the applications to write data of a designated file type to said storage device. Further, that detection can occur using a process operating in kernel mode, as shown below. **How does Intercept X prevent vulnerabilities being exploited** Intercept X monitors classes of applications at the kernel level. This injection into the process allows close and continuous monitoring of activity in the process, including memory access, disk, network access, DLLs loaded, and other process interactions. Intercept X Solution Brief (https://www.avanet.com/assets/pdf/sophos-intercept-x-solution-brief-en.pdf) **Behavior Monitoring and Application Lockdown** Some attackers inject code in trusted applications without spawning child processes. Intercept X can stop these attacks that abuse real software capabilities for destructive purposes. Intercept X classifies applications based on how they are registered with the system; categories include web browsers and plug-ins; java-based applications; media readers, editors, and players; and document creation/reading applications. By monitoring application classes at the kernel level, Intercept X can track activities related to memory access, storage, networks, DLLs, and other software process interactions, and lock down processes as needed. https://www.avanet.com/assets/pdf/sophos-intercept-x-esg-lab-validation-jan-2018-en.pdf at 8

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[a] detecting using a process operating in kernel mode monitoring file system access an attempt by the application to write data of a designated file type to said data storage device;	Below is another example of the detection occurring using a process operating in kernel mode. **Overview** The Talpa on-access scanning component of Sophos anti-virus for Linux requires several kernel modules to be installed and loaded. For ease of installation, Sophos provides pre-compiled Talpa Binary Packs for certain kernel versions. For kernels for which Sophos does not provide a Talpa Binary Pack, or for which Fanotify is not supported, the Sophos anti-virus installer may be able to compile custom Talpa Binary Packs locally to match your running kernel. Instructions are provided below. **Note**: From Sophos anti-virus version 9.7 or later, you can enable on-access scanning using Fanotify on many kernels without loading or compiling a Talpa kernel module. Please see the knowledge base article Sophos Anti-Virus for Linux: Fanotify overview. https://community.sophos.com/kb/en-us/13503

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and	In response to the write attempts discussed for limitation 16[pre] and [a], the Sophos software retrieves a permission value from a database comprised of data elements encoding at least one permission value associated with the application. For example, the Sophos software utilizes rules, policies, whitelists, authorized lists, exceptions, allowed lists, and/or IDE file lists that are stored in a database. For example, Sophos's "Authorized list" includes at lease one permission value (e.g., an authorization) associated with each item on the list, and each item is associated with an application. The programs on the exception list are stored on a database that include data elements encoding permission values, e.g., approved or blocked, that are associated with the applications on the list.

Authorize	Users can authorize suspicious items, adware, and PUAs in order to allow them to run on the computer. This option applies to both **Authorization manager** and **Quarantine manager**.

If you want to allow an item that Sophos Anti-Virus has classified as suspicious, you can authorize it as follows.

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Authorization**.
2. Click the tab for the type of item that has been detected (for example, **Buffer overflow**).
3. In the **Known** list, select the suspicious item.
4. Click **Add**.

The suspicious item appears in the **Authorized** list.

https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 6, 32.

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and	As another example, the Sophos software also includes whitelists. The programs on that list are stored on a database that include data elements encoding permission values, e.g., trusted or not, that are associated with the applications on the list. Further information Given the number of files scanned by Sophos Anti-Virus a look-up can be triggered quite frequently. This is not an event that an end user would see but you may see traffic if monitoring your firewall etc. To limit the number of look-ups SophosLabs also whitelists common files, so they will not be scanned, this includes OS files but also common applications. Due to the nature of malware we attempt to reduce the number of look-ups where possible but do not set an arbitrary limit as we do not want to compromise on the protection we offer customers and the rapid response cloud look-ups. https://community.sophos.com/kb/en-us/111334

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and	As another example, the Sophos software also includes an allow list. The programs on that list are stored on a database that include data elements encoding permission values, e.g., allowed or not, that are associated with the applications on the list. While an allow list is maintained by SophosLabs, the list is provided to and stored in the computer to "improve performance." How does it work? LiveProtection will perform a lookup for any file it suspects of being malware; the following events will trigger a lookup • Whenever a file is added to the endpoint's quarantine manager. • Whenever reported internally by the anti-malware engine that a file is deemed suitably suspicious. • Whenever reported internally by anti-malware engine that a file is to be checked against a allow list defined by SophosLabs. (The allow list is maintained by SophosLabs and contains a list of common and system files which the product should cache to improve performance.) https://community.sophos.com/kb/en-us/110921

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and	As another example, the Sophos software also includes an excluded list. The programs on that list are stored on a database that include data elements encoding permission values, e.g., excluded or not, that are associated with the applications on the list. **5.4.1 Exclude items from on-access scanning** **Important** If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here. To edit the list of files, folders, and drives that are excluded from on-access scanning: 1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning**. 2. Click the **Exclusions** tab, and then choose one of the following options. • To specify a file, folder, or drive that should be excluded from on-access scanning, click **Add**. • To delete an exclusion, click **Remove**. • To change an exclusion, click **Edit**. 3. To add or edit an excluded item, in the **Exclude item** dialog box, select the **Item type**. The **All remote files** item type is for excluding files that are not stored on local drives. You might select this if you want to increase speed of access to such files and you trust the available remote file locations. 4. Specify the **Item name** by using the **Browse** button or typing in the text box. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 21

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and	Below is yet another example of a Sophos list that allows a user to specify which file extension are scanned during on-access scanning. 5.2.6 Specify on-access scanning file extensions **Important** If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here. You can specify which file extensions are scanned during on-access scanning. 1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning**. 2. Click the **Extensions** tab, set the options as described below. **Scan all files** Click this to enable scanning of all files, regardless of the filename extension. **Allow me to control exactly what is scanned** Click this to restrict scanning to only files with a particular filename extension, specified in the extension list. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf at 15

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and	As another example, the Sophos software also includes "threat identify (IDE) files." The programs on that list are stored on a database that include data elements encoding permission values, e.g., trusted or not, that are associated with the applications on the list. **Sophos Live Protection - What is it?** As malware continues to rapidly evolve and grow, Sophos has realized that it needs a way to enhance existing data updates with a system to keep endpoint protection up to date in real-time. This was done to both improve the response time to new malware and reduce the amount of data delivered to the endpoints. LiveProtection was added to give the endpoint the ability to 'lookup' files in real-time to verify if they are malicious. Over the past few years it has proven very effective at stopping new malware outbreaks and protecting our customers. Sophos Live Protection can perform the following tasks: • Perform cloud look-ups against individual files to determine if safe/malicious If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis. This is known as 'in-the-cloud' checking: it performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated. https://community.sophos.com/kb/en-us/110921

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	SOPHOS PRODUCTS
16[c] controlling write access to the data storage device by the application in dependence on said permission value.	As shown in the slides for limitation 16[b], Sophos's Software controls write access to the data storage device by the application in dependence on said permission value. For example, if the application in on an authorized list, white list, or allowed list, or excluded list then the application is allowed write access. Further, if the application is on an IDE file list, the permission value retrieved (as discussed for limitation 16[b]) based on the list will indicate whether to allow or deny write access.